CLAIMS

1. A method of performing policy enforcement by a switch, comprising:

receiving a plurality of frames;

examining at least some of the received frames to determine whether they require non-default policy enforcement according to pre-programmed policy rules which pertain to at least one protocol; and

forwarding, with default policy handling, at least some of the received frames which belong to the protocol to which the rules pertain, regardless of the policy enforcement they require.

2. A method according to claim 1, comprising applying non-default policy enforcement to the examined frames which so require.

3. A method according to claim 1, wherein examining at least some of the received frames to determine whether they require non-default policy enforcement comprises determining whether the at least some of the received frames adhere to user pre-programmed security rules.

4. A method according to claim 3, comprising discarding examined frames which do not adhere to the security rules.

5. A method according to claim 1, wherein examining at least some of the received frames to determine whether they require non-default policy enforcement comprises determining the required quality of service of the frames.

6. A method according to claim 1, wherein examining at least some of the received frames to determine whether they require non-default policy enforcement comprises determining whether the at least some of the received frames require sniffing or counting.

7. A method according to claim 1, wherein examining the at least some of the received frames comprises comparing values of one or more of the fields of the frames to respective fields in a list of policies of groups of frames.

8. A method according to claim 7, wherein forwarding at least some of the frames regardless of the policy enforcement they require comprises forwarding, with default policy handling, non-leading frames of sessions of a connection-based protocol for which no match was found in the comparing to the list.

9. A method according to claim 7, wherein examining at least some of the received frames comprises checking frames for which no match was found in the comparison to the list against the pre-programmed rules.

10. A method according to claim 1, wherein forwarding at least some of the frames regardless of the policy enforcement they require comprises forwarding, with default policy handling, substantially all non-leading frames of sessions of a connection-based protocol.

11. A method according to claim 10, wherein forwarding, with default policy handling, substantially all non-leading frames of sessions of a connection-based protocol comprises forwarding, with default policy handling, substantially all frames starting with the third frame of two-way sessions of a connection-based protocol.

12. A method according to claim 10, wherein forwarding all non-leading frames of sessions of a connection-based protocol comprises forwarding, with default policy handling, substantially all frames starting with the second frame of two-way sessions of a connection-based protocol.

13. A method according to claim 10, wherein the connection-based protocol comprises the TCP protocol.

14. A method according to claim 10, wherein examining at least some of the received frames comprises examining leading frames of sessions of connection based protocols.

15. A method according to claim 10, wherein examining at least some of the received frames comprises examining frames of connectionless protocols.

16. A method according to claim 1, wherein forwarding, with default policy handling, at least some of the frames comprises forwarding, with default policy handling, frames which include IP packets.

17. A method according to claim 1, wherein forwarding, with default policy handling, at least some of the received frames regardless of the policy enforcement they require comprises forwarding, with default policy handling, substantially all the frames received from one or more specific physical ports of the switch.

18. A method according to claim 17, wherein the one or more specific physical ports are connected to switches which perform policy enforcement.

19. A method according to claim 17, wherein the one or more specific physical ports are not connected directly to end-stations.

20. A method according to claim 1, wherein forwarding, with default policy handling, at least some of the received frames regardless of the policy enforcement they require comprises forwarding, with default policy handling, frames received with indications that the frames underwent policy enforcement.

21. A method according to claim 1, wherein forwarding, with default policy handling, at least some of the received frames regardless of the policy enforcement they require comprises forwarding the at least some of the received frames without determining the policy they require.

22. A method according to claim 1, wherein forwarding, with default policy handling, at least some of the received frames regardless of the policy enforcement they require comprises

forwarding at least one frame with a policy different than required by the preprogrammed rules.

23. A method according to claim 1, wherein forwarding, with default policy handling, at least some of the received frames regardless of the policy enforcement they require comprises forwarding, with default policy handling, frames which require policy handling which differs from the default only in the required quality of service.

24. A method of performing policy enforcement by a switch, comprising:

receiving a plurality of frames;

comparing the values of one or more fields of at least some of the plurality of frames to entries of a list;

determining whether to additionally analyze the frames for which no match was found in the comparison;

additionally analyzing at least some of the frames for which no match was found in the comparison; and

forwarding at least some of the frames for which no match was found in the comparison without performing additional analysis.

25. A method according to claim 24, wherein the list identifies frames which may be forwarded without violating security rules.

26. A method according to claim 24, wherein additionally analyzing at least some of the frames for which no match was found in the comparison comprises analyzing those frames belonging to connectionless protocols.

27. A method according to claim 24, wherein additionally analyzing at least some of the frames for which no match was found in the comparison comprises analyzing leading frames of sessions of connection based protocols.

28. A method according to claim 24, wherein the one or more fields comprise source and destination address fields.

29. A method according to claim 24, wherein at least some of the frames are not compared to the entries of the list.

30. A method according to claim 29, wherein leading frames of sessions of connection based protocols are not compared to the entries of the list.

31. A method according to claim 24, wherein forwarding without performing additional analysis comprises forwarding those frames which are non-leading frames of connection based protocol sessions.

32. A method according to claim 24, wherein determining whether to additionally analyze comprises determining based on at least one field not included in the comparison.

33. A method according to claim 24, wherein determining whether to additionally analyze comprises determining the protocol to which the frame belongs.

34. A method according to claim 24, wherein the additional analysis is performed by a separate unit than performs the comparison.

35. A method according to claim 34, wherein the comparison is performed by a hardware unit of the switch and the additional analysis is performed by a processor of the switch.

36. A method according to claim 35, wherein the entries of the list are stored in a storage area of the hardware unit.

37. A method of performing policy enforcement by a switch, comprising:

receiving a plurality of frames;

determining whether to compare the values of one or more fields of at least some of the plurality of frames to entries of a list of policies of groups of frames;

comparing the values of one or more fields of the determined frames to respective fields of entries of the list; and

forwarding, discarding or further analyzing frames determined not to be compared.

38. A method according to claim 37, wherein determining whether to compare comprises determining based on the physical port from which the frame was received.

39. A method according to claim 37, wherein determining whether to compare comprises determining based on the protocol of the frame.

40. A method according to claim 37, wherein further analyzing comprises transferring to a processor of the switch.

41. A switch for forwarding frames, comprising:

at least one port which receives frames; and

a table which includes entries which list policies of groups of frames, and indicates for at least one of the entries different behavior for leading and non-leading frames of sessions matching the entry.

42. A switch according to claim 41, comprising a hardware unit which forwards the non-leading frames of sessions matching the at least one of the entries which indicate different behavior for leading and non-leading frames, without further analysis.

43. A switch according to claim 41, comprising a processor which analyzes the leading frames of sessions matching the at least one of the entries which indicate different behavior for leading and non-leading frames.

44. A switch according to claim 41, wherein each entry of the table matches frames of a plurality of sessions.

45. A switch for forwarding frames, comprising:

at least one port which receives frames;

a table which includes entries which list policies of groups of frames; and

a hardware unit which compares the values of one or more fields of at least some of the received plurality of frames to entries of the table and forwards with a default policy at least some of the frames for which no match was found in the comparison.

46. A switch according to claim 45, comprising a processor which analyzes at least some of the frames for which no match was found in the comparison.

47. A switch according to claim 45, wherein the policy table comprises a plurality of groups of entries with different key fields.

48. A switch according to claim 45, wherein the policy table comprises at least one field which receives wildcard values.

49. A method of performing policy enforcement by a switch, comprising:

receiving a plurality of frames;

comparing at least some of the received frames to a list of groups of frames and respective policies; and

creating entries in the list for less than all of the compared frames for which no match was found in the comparison to the list.

50. A method according to claim 49, wherein creating entries in the list for less than all of the compared frames comprises creating entries only for frames received through physical ports connected directly to end-stations.

51. A method according to claim 49, wherein creating entries in the list for less than all of the compared frames comprises creating entries only for frames belonging to connectionless protocols.

52. A method according to claim 49, wherein creating entries in the list for less than all of the compared frames comprises not creating entries for at least some of the frames which require a policy which differs from a default policy only in quality of service.

53. A method according to claim 49, wherein creating entries in the list for less than all of the compared frames comprises not creating entries for at least some of the frames which require a policy which differs from a default policy only in tasks other than quality of service.

54. A method according to claim 49, comprising determining, for the compared frames, a probability that additional frames of the same session will be received by the switch and creating entries only for frames with a probability higher than a predetermined level.

55. A method of forwarding a frame by a switch, comprising:

receiving a frame;

checking one or more layer-3 or above fields of the frame for adherence to security rules; and

performing layer-2 hardware switching of the frame, if the frame adheres to the security rules.

56. A method according to claim 55, wherein performing layer-2 switching of the frame comprises forwarding without changing a destination MAC address of the frame.

57. A method according to claim 55, wherein checking the frame for adherence to security rules comprises checking by a hardware unit.

58. A method according to claim 55, wherein performing layer-2 switching of the frame comprises forwarding without changing a source MAC address of the frame.

59. A method according to claim 55, wherein checking for adherence to security rules comprises checking by a hardware unit.

60. A switch for forwarding frames, comprising:

at least one port which receives frames;

a security unit which checks the received frames for adherence to security rules; and

a forwarding unit which performs layer-2 switching of frames which adhere to the security rules.

61. A switch according to claim 60, wherein the security unit comprises a policy table which has a plurality of entries to which the received frames are compared.

62. A switch according to claim 61, wherein the switch has at least one group of eight ports and the policy table has room for up to 256 entries for each group of eight physical ports of the switch.

63. A switch according to claim 60, wherein the switch cannot perform layer-3 routing.

64. A switch according to claim 60, wherein the security unit comprises a hardware unit.

65. A switch for forwarding frames, comprising:

at least one port which receives frames;

a policy table which includes entries, addressed by at least two key fields, for sessions which should receive non-default policy behavior;

a policy unit which checks whether at least some of the received frames which do not have respective entries in the policy table require non-default policy behavior; and

a forwarding unit which performs layer-2 switching of the at least some of the received frames in accordance with the policy behavior determined by the policy unit.

66. A switch according to claim 65, wherein the policy unit also checks whether received frames which have respective entries in the policy table require non-default policy behavior.

67. A switch according to claim 66, wherein the policy unit comprises a hardware unit which checks received frames which have respective entries and a processor which checks received frames which do not have respective entries in the table.

68. A switch according to claim 66, wherein the entries of the table are addressed by at least the IP source and destination addresses of the received frames.

69. A switch according to claim 66, wherein the entries of the table each define a single session.

70. A method of updating a policy table of a switch, comprising:

receiving a frame which is not directed to the switch;

creating an entry in the policy table of the switch, for the session to which the received frame belongs; and

performing layer-2 switching of the received frame.

71. A method according to claim 70, comprising determining whether the received frame requires non-default policy enforcement, and creating the entry is performed only if the received frame requires non-default policy enforcement.

72. A method according to claim 71, wherein the received frame belongs to a connection-based protocol.

73. A method according to claim 71, wherein determining whether the received frame requires non-default policy enforcement comprises checking whether the frame requires sniffing.

74. A method according to claim 71, wherein determining whether the received frame requires non-default policy enforcement comprises checking whether the frame belongs to a group which requires frame counting.

75. A method according to claim 71, wherein determining whether the received frame requires non-default policy enforcement comprises checking whether the frame violates security rules.

76. A method according to claim 71, wherein determining whether the received frame requires non-default policy enforcement comprises checking whether the frame requires a non-default QoS behavior.

77. A method according to claim 70, wherein receiving the frame comprises receiving a frame which does not relate to the same session as addressed by any recently received control message.

78. A packet based network, comprising:

a plurality of at least three switches which perform layer-2 switching of frames;

one or more links which connect the plurality of switches to each other,

at least 50% of the switches comprising a policy unit which performs policy enforcement on at least some of the frames transmitted within the network.

79. A network according to claim 78, wherein substantially all the switches in the network comprise a policy unit which performs policy enforcement on at least some of the frames transmitted within the network.

80. A network according to claim 78, wherein at least some of the policy units of the switches perform different groups of policy enforcement tasks.